Claims

1. A method for providing authentication for setting up secure connections between a plurality of network nodes comprising at least the steps of

- placing a collection of accepted certificates comprising at least one accepted certificate available for other nodes by said first node,

- importing said collection by at least one other node than said first node,

- setting up of at least one secure connection by at least one of said at least one other node to a destination node whose certificate was imported as a part of said collection, and automatically accepting the authenticity of said destination node.

2. A method according to claim 1 further comprising at least the steps of

- automatically obtaining a certificate of a second node by a first node,

- displaying at least an identification string of said certificate to the user of said first node,

- receiving an indication of acceptance or rejection of trust regarding said certificate from said user, and in the case of receiving an indication of acceptance, storing at least an indication of the acceptance and said certificate, and

- setting up a secure connection from said first node to said second node.

3. A method according to claim 1 further comprising at least the step of digitally signing said collection by said first node.

4. A method according to claim 1 further comprising at least the steps of encryption of said collection by said first node.

5. A method according to claim 1 further comprising at least the step of saving certificate use policy information in said collection by said first node.

6. A method according to claim 1 further comprising at least the step of digitally signing each certificate in said collection by said first node.

7. A method in a network node for setting up secure connections between the node and other network nodes comprising at least the steps of

- automatically obtaining a certificate of a second node by the network node,

- displaying at least an identification string of said certificate to the user of the network node,

- receiving an indication of acceptance or rejection of trust regarding said certificate from said user, and in the case of receiving an indication of acceptance, storing at least an indication of the acceptance and said certificate,

- setting up a secure connection from the network node to said second node, and

- placing a collection of accepted certificates comprising at least one accepted certificate available for other nodes by the network node.

8. A method in a network node for setting up secure connections between the node and other network nodes comprising at least the steps of

- importing a collection of accepted certificates from at least one other node,

- setting up of at least one secure connection to a destination node whose certificate was imported as a part of said collection, and automatically accepting the authenticity of said destination node.

9. A system in a network node for setting up secure connections between network nodes comprising at least

- means for placing a collection of accepted certificates comprising at least one accepted certificate available for other nodes,

- means for importing a collection of accepted certificates from another node,

- means for setting up of at least one secure connection to a destination node, and

means for automatically accepting the authenticity of a destination node, if the certificate of said destination node was previously imported by said means for importing.

10. A computer program product for setting up secure connections between network nodes comprising at least

- computer program code means for placing a collection of accepted certificates comprising at least one accepted certificate available for other nodes,

- computer program code means for importing a collection of accepted certificates from another node,

- computer program code means for setting up of at least one secure connection to a destination node, and

- computer program code means for automatically accepting the authenticity of a destination node, if the certificate of said destination node was previously imported by said means for importing.

11. A computer program product according to claim 10 further comprising firewall functionality.

12. A computer program product according to claim 10 wherein the computer program product is an IPSec client program.

13. A computer program product according to claim 10, further comprising

- computer program code means for obtaining a certificate of a remote node,

- computer program code means for displaying at least an identification string of said certificate to the user of the computer program product,

- computer program code means for receiving an indication of acceptance or rejection of trust regarding said certificate from said user, and

- computer program code means for storing at least an indication of the acceptance and said certificate in the case of receiving an indication of acceptance.

14. A computer in a network having network nodes comprising at least

- computer program code means for placing a collection of accepted certificates comprising at least one accepted certificate available for other nodes,

- computer program code means for importing a collection of accepted certificates from another node,

- computer program code means for setting up of at least one secure connection to a destination node, and

computer program code means for automatically accepting the authenticity of a destination node, if the certificate of said destination node was previously imported by said means for importing.

15. A method for automatic configuration of a network node, wherein the method comprises at least the steps of

- initiating a negotiation according to a security parameter negotiation protocol with a second network node,
- sending a request for a certificate,
- receiving a certificate,
- terminating said negotiation, and
- determining a connection parameter value based at least in part on information received during said negotiation.

16. A method according to claim 15 further comprising the step of determining a parameter value based at least in part on information in said received certificate.

17. A method according to claim 15 further comprising the step of determining a parameter value based at least in part on manufacturer identification information received from said second network node.

18. A method according to claim 15 further comprising the steps of
- determining if a packet has been modified during transit from said second node, and
- determining a parameter value based on the result of said determining if a packet has been modified.

19. A method according to claim 15 wherein said protocol is the IKE protocol.